UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,176	06/24/2003	Christian Gehrmann	P17725-US2	9477

27045 7590 12/22/2006

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/22/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/602,176	GEHRMANN, CHRISTIAN	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see attached*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for domestic priority under 35 U.S.C. 119(e).

Information Disclosure Statement

2. The information disclosure statements submitted are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-8,10-17,19-22,24-28, and 30-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Jablon, U.S. Patent 6,226,383.

As per claim 1, Jablon teaches of a method of providing secure communications between a first and a second communications unit, the method comprising a key exchange between the first and second communications units resulting in a shared secret key, the key exchange including a user interaction, the method comprising the

steps of providing, at least partly by means of a user interaction, a passcode to the first and second communications units; generating a first contribution to the shared secret key by the first communications unit and a second contribution to the shared secret key by the second communications unit, and transmitting each generated contribution to the corresponding other communications unit; authenticating the transmitted first and second contributions by the corresponding receiving communications unit based on at least the passcode; and establishing said shared secret key by each of the communications units from at least the corresponding received first or second contribution, only if the corresponding received contribution is authenticated successfully (col. 6, lines 56-60; col. 6, line 66 through col. 7, line 31; and col. 8, line 55 through col. 9, line 12).

As per claim 2, Jablon discloses wherein the passcode is short enough to be communicated via a user interaction (col. 8, lines 55-59).

As per claim 3, it is taught by Jablon of encrypting the passcode by the second communications unit using the generated shared secret key; transmitting the encrypted passcode to the first communications unit together with the generated second contribution; decrypting the received encrypted passcode by the first communications unit; and comparing the decrypted received passcode with the passcode provided to the first communications unit to authenticate the received second contribution (col. 6, lines 56-60 and col. 6, line 66 through col. 7, line 31).

As per claim 4, it is disclosed by Jablon wherein the first and second contributions are first and second public keys of a Diffie-Hellman key exchange protocol (col. 7, lines 1-7).

As per claim 5, Jablon teaches wherein the step of providing a passcode to the first and second communications units comprises generating a passcode by the first communications unit and providing the generated passcode to the second communications unit via a communications channel including a user interaction (col. 6, lines 56-60 and col. 6, line 66 through col. 7, line 31).

As per claim 6, Jablon discloses wherein the step of authenticating the transmitted first and second contributions comprises authenticating the first contribution by calculating a tag value of a message authentication code, the tag value being calculated from the first contribution and the passcode (col. 6, line 66 through col. 7, line 31 and col. 22, lines 23-34).

As per claim 7, it is taught by Jablon wherein the tag value is calculated by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the first contribution, and the symbol being identified by the passcode (col. 6, line 66 through col. 7, line 31 and col. 22, lines 23-34).

As per claim 8, it is disclosed by Jablon of calculating a hash value of a one-way hash function from the first contribution and calculating said tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the hash value of the first contribution, and the symbol being identified by the passcode (col. 15, lines 10-16 and col. 22, lines 23-34).

As per claim 10, Jablon discloses of generating the first contribution to the shared secret key by the first communications unit, and transmitting the generated first contribution to the second communications unit; authenticating the received first contribution by the second communications unit based on the passcode, and generating the shared secret key from at least the received first contribution, if the received first contribution is accepted as authentic; transmitting a second contribution to the shared secret key generated by the second communications unit to the first communications unit; and authenticating the received second contribution by the first communications unit based on the passcode; and generating the shared secret key by the second communications unit only if the received first contribution is accepted as authentic (col. 6, line 66 through col. 7, line 31).

As per claim 11, it is taught by Jablon wherein the method further comprises calculating a first message tag of a message authentication code from the first contribution using the passcode as a key; and providing the calculated first message tag to the second communications unit; and wherein the step of authenticating the received first contribution by the second communications unit based on the passcode comprises calculating a second message tag of said message authentication code from the received first contribution using the passcode as a key; and comparing the first and second message tag to authenticate the received first contribution (col. 6, line 66 through col. 7, line 31).

As per claim 12, it is disclosed by Jablon of a method of providing secure communications between a first communications unit and a second communications

unit, the method comprising a registration step and a key exchange step, wherein the registration step comprises generating a first private key value and a corresponding first public key of a key exchange mechanism by the first communications unit; generating a passcode by the first communications unit; calculating a message tag of the first public key according to a message authentication code using the passcode by the first communications unit; making the passcode and the calculated tag value accessible to the second communications unit at least partly by means of a user interaction; and the key exchange step comprises transmitting the first public key by the first communications unit to the second communications unit; calculating the tag value of the received first public key according to said message authentication code using the passcode by the second communications unit, and accepting the received first public key if the calculated tag value corresponds to the communicated tag value; generating a second private key value and a corresponding second public key of said key exchange mechanism by the second communications unit; calculating a shared secret key of said key exchange mechanism from the first public key and the second private key value by the second communications unit; encrypting the passcode by the second communications unit using the calculated shared secret key; transmitting the second public key and the encrypted passcode by the second communications unit to the first communications unit; calculating said shared secret key of said key exchange mechanism from the second public key and the first private key value by the first communications unit; and decrypting the transmitted encrypted passcode by the first communications unit using the shared secret key calculated by the first communications

unit, and accepting the calculated shared secret key if the decrypted passcode corresponds to the passcode originally generated by the first communications unit (col. 6, lines 56-60; col. 6, line 66 through col. 7, line 31; and col. 8, line 55 through col. 9, line 12).

As per claim 13, Jablon teaches of a communications system for providing secure communications at least between a first and a second communications unit by means of a key exchange between the first and second communications units resulting in a shared secret key, the key exchange including a user interaction, the communications system comprising means for providing, at least partly by means of a user interaction, a passcode to the first and second communications units; means for generating a first contribution to the shared secret key by the first communications unit and a second contribution to the shared secret key by the second communications unit; means for transmitting each generated contribution to the corresponding other communications unit; means for authenticating the transmitted first and second contributions by the corresponding receiving communications unit based on the passcode; and means for establishing said shared secret key by each of the communications units from at least the corresponding received first or second contribution, only if the corresponding received contribution is authenticated successfully (col. 6, lines 56-60; col. 6, line 66 through col. 7, line 31; and col. 8, line 55 through col. 9, line 12).

As per claim 14, Jablon discloses wherein the first communications unit comprises processing means adapted to generate the passcode and output means for

providing the generated passcode to the second communications unit via a second communications channel different from the first communications channel (col. 6, line 66 through col. 7, line 31).

As per claim 15, it is taught by Jablon wherein the first and second communications units each comprise processing means for calculating a tag value of a message authentication code, the tag value being calculated from the first contribution and the passcode (col. 6, line 66 through col. 7, line 31 and col. 22, lines 23-34).

As per claim 16, it is disclosed by Jablon wherein the processing means are adapted to calculate the tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the first contribution, and the symbol being identified by the passcode (col. 6, line 66 through col. 7, line 31 and col. 22, lines 23-34).

As per claim 17, Jablon teaches wherein the processing means are further adapted to calculate a hash value of a one-way hash function from the first contribution and to calculate said tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the hash value of the first contribution, and the symbol being identified by the passcode (col. 15, lines 10-16 and col. 22, lines 23-34):

As per claim 19, it is taught by Jablon of a communications unit for providing secure communications with another communications unit by means of a key exchange resulting in a shared secret key, the key exchange including a user interaction, the communications unit comprising data processing means, user-interface means, and a

communications interface, the processing means being adapted to perform the following steps generating a passcode to be provided at least partly by means of a user interaction via the user-interface means, to the other communications unit; generating and transmitting via the communications interface a first contribution to the shared secret key, and receiving via the communications interface a second contribution to the shared secret key, the second contribution being generated by the other communications unit; authenticating the received second contribution based on the passcode; and establishing said shared secret key from at least the second contribution, only if the received second contribution is authenticated successfully (col. 6, lines 56-60; col. 6, line 66 through col. 7, line 31; and col. 8, line 55 through col. 9, line 12).

As per claim 20, it is disclosed by Jablon wherein the processing means is further adapted to calculate a tag value of a message authentication code to be provided to the other communications unit, the tag value being calculated from the first contribution and the passcode (col. 6, line 66 through col. 7, line 31 and col. 22, lines 23-34).

As per claim 21, Jablon teaches wherein the processing means is further adapted to calculate the tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the first contribution, and the symbol being identified by the passcode (col. 6, line 66 through col. 7, line 31 and col. 22, lines 23-34).

As per claim 22, Jablon discloses wherein the processing means is further adapted to calculate a hash value of a one-way hash function from the first contribution

and to calculate said tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the hash value of the first contribution, and the symbol being identified by the passcode (col. 6, line 66 through col. 7, line 31 and col. 22, lines 23-34).

As per claim 24, it is disclosed by Jablon wherein the processing means is further adapted to decrypt an encrypted passcode received together with the second contribution, the decrypting using said shared secret key, and is further adapted to accept the received second contribution only if the decrypted passcode corresponds to the generated passcode (col. 6, lines 56-60 and col. 6, line 66 through col. 7, line 31).

As per claim 25, Jablon teaches of a communications unit for providing secure communications with another communications unit by means of a key exchange resulting in a shared secret key, the key exchange including a user interaction, the communications unit comprising data processing means, storage means, and a communications interface, the processing means being adapted to perform a key exchange resulting in a shared secret key, the key exchange comprising: receiving, at least partly by means of a user interaction, and storing a passcode generated by another communications unit; receiving via the communications interface a first contribution to the shared secret key generated by the other communications unit; authenticating the received first contribution based on the passcode; and if the received first contribution is authenticated successfully, establishing said shared secret key from at least the first contribution, and transmitting via the communications interface a

second contribution to the shared secret key (col. 6, lines 56-60; col. 6, line 66 through col. 7, line 31; and col. 8, line 55 through col. 9, line 12).

As per claim 26, Jablon discloses of being adapted to store a message authentication tag in the storage means, and wherein the processing means is adapted to calculate a tag value of a message authentication code from the received first contribution and the passcode, and is adapted to accept the received first contribution only of the calculated tag value corresponds to the stored message authentication tag (col. 6, line 66 through col. 7, line 31 and col. 22, lines 23-34).

As per claim 27, it is taught by Jablon wherein the processing means is further adapted to calculate the tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the first contribution, and the symbol being identified by the passcode (col. 6, line 66 through col. 7, line 31 and col. 22, lines 23-34).

As per claim 28, it is disclosed by Jablon wherein the processing means is further adapted to calculate a hash value of a one-way hash function from the first contribution and to calculate said tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the hash value of the first contribution, and the symbol being identified by the passcode (col. 15, lines 10-16 and col. 22, lines 23-34

As per claim 30, Jablon discloses wherein the processing means is further adapted to encrypt the stored passcode, the encrypting using said shared secret key, and is further adapted to transmit the encrypted passcode with the second contribution

via the communications interface to the other communications unit (col. 6, line 66 through col. 7, line 31).

As per claim 31, it is taught by Jablon of a computer program product configured to provide secure communications between a first and a second communications unit, comprising a computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising: computer readable program code for exchanging a key between the first and the second communications units to generate a shared secret key and to receive input from a user; computer readable program code for providing, at least partly by means of a user interaction, a passcode to the first and second communications units; computer readable program code for generating a first contribution to the shared secret key by the first communications unit and a second contribution to the shared secret key by the second communications unit, and transmitting each generated contribution to the corresponding other communications unit; computer readable program code for authenticating the transmitted first and second contributions by the corresponding receiving communications unit based on at least the passcode; and computer readable program code for establishing said shared secret key by each of the communications units from at least the corresponding received first or second contribution, only if the corresponding received contribution is authenticated successfully (col. 6, lines 56-60; col. 6, line 66 through col. 7, line 31; and col. 8, line 55 through col. 9, line 12).

As per claim 32, it is disclosed by Jablon of a computer program product configured to provide secure communications with a communications unit, comprising a

computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising: computer readable program code for exchanging a key with the communication unit to generate a shared secret key and to receive input from a user; computer readable program code for generating a passcode to be provided based on user input to the communication unit; computer readable program code for generating and transmitting a first contribution to the shared secret key, and receiving a second contribution to the shared secret key, the second contribution being generated by the communication unit; computer readable program code for authenticating the received second contribution based on the passcode; and computer readable program code for establishing the shared secret key from at least the second contribution, based on whether the received second contribution is authenticated (col. 6, lines 56-60; col. 6, line 66 through col. 7, line 31; and col. 8, line 55 through col. 9, line 12).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 9,18,23, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon, U.S. Patent 6,226,383.

The teachings of Jablon disclose of using a message authentication code, but fail to disclose of the use of Reed-Solomon code. The examiner hereby takes official notice that it is notice that it is a notoriously well known form of error correcting code. It would have been obvious to a person of ordinary skill in the art at the time of invention to have been motivated to apply the use of Reed-Solomon code. The motivation for using Reed-Solomon is that sampling is performed at various points in the code for error checking purposes to maintain the integrity of the code. It would have been obvious to use Reed-Solomon code in an attempt to detect errors in the transmitted code.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CR

December 20, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER